

Gateway Redundancy Using Common Address Redundancy Protocol (CARP)

Rini Nur¹, Zawiyah Saharuna², Irmawati³, Irawan⁴, Reski Wahyuni⁵

Abstract—Gateway redundancy can ensure the network availability and reliability in providing a service. One way is to make a backup system on the gateway. This backup system can be applied to the router so that if a failure occurs on the master router its task and function can be transferred to the slave router. The transition process from master router to slave router is known as failover. Common Address Redundancy Protocol (CARP) is one of the redundancy gateway protocols and provides a failover mechanism on the router. Therefore, this study will analyse the CARP protocol implementation in ensuring the network services availability by measuring parameters of throughput, delay, retransmission, and downtime. The results showed that CARP implementation on the network produced the throughput, delay, and retransmission values of 61.7 Mbps, 0.14 ms, and 1.11% when without the link termination and 18 Mbps, 0.53 ms, and 1.58% when with link termination, while the downtime value is 2.91 seconds. The QoS test results show good quality based on ITU-T.

Keywords — CARP, redundancy, gateway, failover.

I. INTRODUCTION

The survey conducted by the Indonesian Internet Service Providers Association (APJII) in 2016 resulted in as many as 132.7 million Indonesians has already been connected to the internet. This shows that there has been an increase of 51.8% internet users compared to 2014 with a total of 88.1 million [1]. The increase in the number of internet users in Indonesia has led to increased demand for service quality improvement. Internet networks availability and reliability levels are very important in accelerating data communication [2].

To ensure a high availability and high reliability network can be done by building a backup system on network components so as to minimize the failure occurrence at one point (Single Point of Failure). The addition of a backup system is known as redundancy [3].

One of redundancy technologies important to be implemented is the gateway redundancy. At the gateway redundancy the main concern lies in the router device. Failure of one connection point on the router will result in a network connection disconnection. Therefore, it is very necessary to add a backup router as a redundancy device to maintain the connections availability on the gateway network [4].

Connection availability occurs because of an automatic transition process, called as failover, between router devices thereby minimizing network connection failures.

One of the redundancy systems on the gateway network that can be used is the Common Address Redundancy Protocol (CARP). CARP was selected because it can guarantee the network services availability by building a backup system and providing a failover mechanism in the network. The failover mechanism in CARP is shorter than VRRP, which is an average of 5 seconds, while VRRP averages is of 7 seconds. CARP implementation is able to pass a maximum throughput of 6 Mbps when a failover occurs with an average packet loss of 5% to 6% [5].

In addition, the CARP implementation to increase network reliability had also been successfully administered in 2016. Research results show that master router failover process to backup router requires ± 3.9 seconds [6].

Based on the description above, then in this paper a redundancy network using CARP is implemented so that it can increase network availability. This paper does not only analyse the CARP mechanism and its failover process as in previous studies, [5], [6], but also analyses CARP's performance which includes throughput, delay, retransmission, and downtime based on ITU-T standards.

II. REDUNDANCY GATEWAY

A. Network Redundancy

Network Redundancy is a way to increase availability, network performance, and minimize single point of failure by duplicating utilized network components. Redundancy also means adding duplicate links or network devices to minimize downtime. These components can be routers, switches, connectivity between devices, Channel Service Unit (CSU), power supply, WAN trunk channels, internet connections, and others. Failure at one connection point on the router will result in network connection disconnection.

There are several redundancy technologies that can be applied to networks, one of which is the gateway redundancy or First Hop Redundancy Protocol (FHRP) [7]. Gateway redundancy consists of Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Gateway Load Balancing Protocol (GLBP), and Common Address Redundancy Protocol (CARP).

B. Common Address Redundancy Protocol (CARP)

CARP is a protocol that allows several identical network segments to share the same IP Address. The CARP protocol can be used on IPv4 and IPv6, and uses the HMAC SHA-1 scheme to check the advertisement integrity and authenticity [8]. This is what protects data in CARP packages because it

¹ Lecturer, Ujung Pandang State Polytechnic, Jl. Perintis Kemerdekaan KM 10 Tamalanrea Makassar 90245 (phone: 0411-585 365; fax: 0411-586043; e-mail: rininur@poliupg.ac.id)

^{2,3,4} Lecturers, Computer and Network Engineering Study Programs, Ujung Pandang State Polytechnic Electrical Engineering Department, Jl. Perintis Kemerdekaan KM 10 Tamalanrea Makassar 90245 (phone: 0411-585 365; fax: 0411-586043; e-mail: zawiyah@poliupg.ac.id)

uses symmetric encryption so that the cluster information confidentiality such as virtual IP address is maintained [9].

In CARP, each node has three parameters to make it work. The first two are advertisement base (advbase) and advertisement skew (advskew). Both affect the time interval the transmitted advertisement [10]. Advskew variable is used to select a master in a redundancy group with the provision that the lower the value of advskew, the higher the priority to become a master. The default value for Advskew is 0 (the range of values that can be used is 0-254). The advbase variable determines how often to initiate itself in seconds to redundancy members. The default value for advbase is 1 second (value range that can be used is 1-255). This variable is used to calculate time duration in seconds when the CARP advertisement is transmitted. This variable determines priority to be a master. The third parameter is the password used to prove / validate the advertisement [9]. CARP used the same IP multicast as VRRP with IP addresses 224.0.0.18 and L2 multicast addresses 01: 00: 5e: 00: 00: 12 to communicate between nodes through advertisement delivery [11].

C. Quality of Service (QoS)

Quality of Service (QoS) is a network ability to provide better services to certain data traffic on various technology platforms types. QoS is not directly obtained from the existing infrastructure, but is obtained by implementing it on the pertinent network [12]. QoS is designed to help users to be more productive by ensuring that users get reliable performance from network-based applications [13]. QoS parameters are throughput, delay, retransmission, and downtime.

Throughput is the actual ability of a network in transmitting data. Usually throughput is always associated with bandwidth because throughput can also be called as bandwidth in actual conditions. Bandwidth is more permanent, while throughput is dynamic depending on ongoing traffic [14].

Delay is the delay time for all packets successfully sent from a source node to a destination node [15]. Time delay affects service quality (QoS) because it causes a packet to reach its destination in longer time. The service quality classification based on ITU-T G.114 consists of three categories, i.e. "good" for 0-150 ms, "sufficient" for 150-400 ms, and "bad" for > 400 ms.

Retransmission is sending back a damaged or missing package. Retransmission is one of the basic mechanisms used by protocols operating through packet switched computer networks to provide reliable communications such as the Transmission Control Protocol (TCP).

Downtime is the period of time when the system cannot be used to carry out its functions as expected. Downtime greatly affects the device availability value [16]. The long downtime amount on the network greatly affects performance and losses in terms of cost.

III. METHODOLOGY

In this paper a network protocol was proposed, it can do redundancy to routers on the gateway network so that it can increase network reliability.

A. System Designing

At this stage the topology used in the research was designed, i.e. the gateway network topology. The topology is shown in Fig. 1 and a list of device IP addresses is presented in Table I.

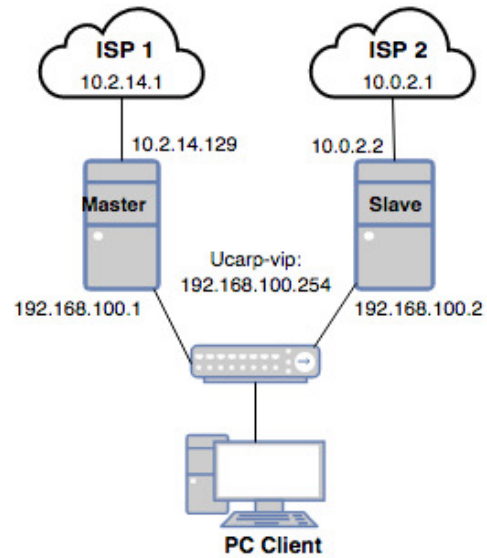


Fig. 1 CARP network topology.

TABLE I
LIST OF CARP NETWORK TOPOLOGY IP ADDRESS

Device	Interface	IP Address (subnet / 24)	Gateway
Router Master	Eth0	10.2.14.129	10.2.14.1
	Eth4	192.168.100.1	
	Ucarp-VIP	192.168,100,254	
Slave Router	Eth1	10.0.2.2/24	10.0.2.1
	Eth2	192.168.100.2	
	Ucarp-VIP	192.168,100,254	
Client PC	LAN-Ether-net	192.168.100.3	192.168,100,254

CARP network topology consisted of two routers, i.e. master and slave routers, and 1 PC as a client. The master router was connected to ISP 1, while the slave router was connected to ISP 2. The bandwidth to ISP 1 was greater than to ISP 2. In normal network conditions, incoming and outgoing network data flows through the master router and ISP 1, while the slave router is used as a backup if there is a failure on the path or the master router device. The virtual IP address used by CARP (UCARP) was 192.168,100.254.

B. Installation and Configuration

At this stage the installation and configuration of the two PC routers were carried out as in Fig. 2. Both routers used the Debian Linux operating system to support CARP implementation. Then the IP address configuration, UCARP (CARP protocol application in Linux OS), and NAT were administered.

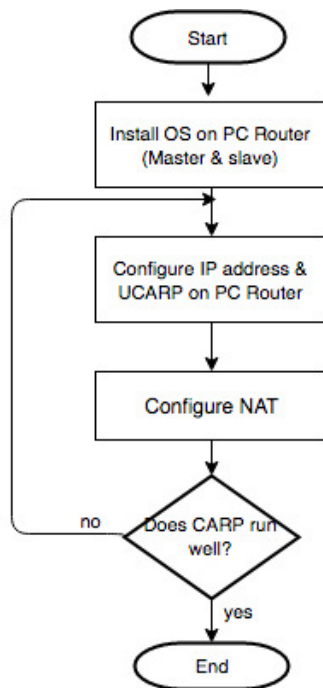


Fig. 2 Network installation and configuration flowchart.

C. Testing Scenario

System testing aimed to ensure the system was running well. Furthermore, an analysis of the data obtained from several test scenarios was administered to obtain information that could be evaluated to suit the objectives to be achieved.

CARP protocol test consisted of two test scenarios, namely:

1. CARP activity test, and
2. qoS parameter test.

CARP activity test was administered when the network was in normal condition, to ensure that CARP had ran well on the gateway network. CARP activity could be seen in router log that stored all activity records from the router.

QoS parameter test was intended to see network performance after CARP was applied in gateway. Therefore, QoS parameter measurements were performed when the CARP network was running normally or without link termination and when a link was terminated from the client to the master router. The QoS parameters to be measured were throughput, delay, retransmission, as well as downtime, and measurements used the Wireshark application. Wireshark recorded data packages on the client side when downloading

files from the internet was done. The format and size of downloaded files were PDF (100.5MB), MKV (215.9MB), and ISO (595MB).

IV. RESULTS AND DISCUSSION

A. CARP Activity Test Results

CARP protocol activities recorded in the log router could be filtered using **fgrep ucarp /var/log/syslog command**. The log shows that UCARP provided information about MAC addresses as a form of advertise into the local network. When the CARP protocol first worked, the router status was still a backup, and it became the master router when there was a status change from backup to master status. This change automatically occurred due to the router's initial configuration as a master router, by giving an advskew and advbase value lower than the slave router, so it had a priority to become a master.

To ensure that the CARP protocol had worked on the master router, the tcpdump command and the Wireshark application were used and the results are shown in Fig. 3 and Fig. 4.

The tcpdump test results showed that the master router had successfully run the CARP protocol which was marked by the advertisement transmitting process. In Fig. 4 it can be seen that the master router runs CARP protocol version 2 with the vhid, advbase, and advskew values on the master router equal to 1.

The Wireshark recordings show router master advertisement activities using the source address 192.168.100.1 and destination address 224.0.0.18 (MAC address 01:00:5e:00:00:12). Address 224.0.0.18 was the CARP protocol multicast address used by the master router to communicate with redundancy members.

B. QoS Parameter Test Results

QoS parameters tests in the form of throughput, delay, retransmission, and downtime were carried out in two conditions, i.e. when the network was normal or without link termination and when there was a link termination from the client toward the master router.

Throughput measurement aimed to determine a network's actual ability in sending data per unit time after the CARP implementation. Throughput results measurements when downloading the various file formats in a normal network and when the link was terminated are shown in Table II.

```

root@master:/home/master# tcpdump -i eth4 -T carp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth4, link-type EN10MB (Ethernet), capture size 262144 bytes
17:49:27.171495 IP master > vrrp.mcast.net: CARPv2-advertise 36: vhid=1 advbase=1 advskew=1 authlen=7 counter=75421
17:49:28.175573 IP master > vrrp.mcast.net: CARPv2-advertise 36: vhid=1 advbase=1 advskew=1 authlen=7 counter=75421
17:49:29.179652 IP master > vrrp.mcast.net: CARPv2-advertise 36: vhid=1 advbase=1 advskew=1 authlen=7 counter=75421
17:49:30.183737 IP master > vrrp.mcast.net: CARPv2-advertise 36: vhid=1 advbase=1 advskew=1 authlen=7 counter=75421
  
```

Fig. 3 Tcpdump master router.

Time	Source	Destination	Protocol	Length	Info
1 2018-04-13 18:09:27.392251	192.168.100.1	224.0.0.18	VRRP	70	Announcement (v2)
2 2018-04-13 18:09:28.392310	192.168.100.1	224.0.0.18	VRRP	70	Announcement (v2)
3 2018-04-13 18:09:29.392341	192.168.100.1	224.0.0.18	VRRP	70	Announcement (v2)
4 2018-04-13 18:09:30.392361	192.168.100.1	224.0.0.18	VRRP	70	Announcement (v2)
5 2018-04-13 18:09:31.392371	192.168.100.1	224.0.0.18	VRRP	70	Announcement (v2)
6 2018-04-13 18:09:32.392413	192.168.100.1	224.0.0.18	VRRP	70	Announcement (v2)
7 2018-04-13 18:09:33.392456	192.168.100.1	224.0.0.18	VRRP	70	Announcement (v2)
8 2018-04-13 18:09:34.392515	192.168.100.1	224.0.0.18	VRRP	70	Announcement (v2)

Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: Icanian_00:00:01 (00:00:5e:00:00:01), Dst: IPv4mcast_12 (01:00:5e:00:00:12)
 Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.18

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
 Total Length: 56
 Identification: 0x0b28 (2856)
 > Flags: 0x4000, Don't fragment
 Time to live: 255
 Protocol: VRRP (112)
 Header checksum: 0x6b61 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.100.1
 Destination: 224.0.0.18

Fig. 4 CARP protocol activities recorded on Wireshark.

TABLE II
THROUGHPUT MEASUREMENT RESULTS

Test Number	Without Link Termination (Mbps)			With Link Termination (Mbps)		
	PDF	MKV	ISO	PDF	MKV	ISO
1	61.68	48.3	49.3	9.8	13.2	26
2	65.6	45.4	51.1	12.5	12.1	23.4
3	57.88	61.4	80.2	12.9	27	30.1
4	61.81	74.6	67.4	13.5	11.7	30.9
5	48.62	77.2	75.2	9.1	14.9	22.9
Average	59.1	61.4	64.6	11.56	15.78	26.66

In Table II it can be seen that measured throughput average value without any link termination is 59.1 Mbps for PDF files, 61.4 Mbps for MKV files, and 64.6 Mbps for ISO files. While the average throughput value when a link was terminated is 11.56 Mbps for PDF files, 15.78 Mbps for MKV files, and 26.66 Mbps for ISO files. The average throughput value for the download process for the three file types is 61.7 Mbps when there was no link termination and 18 Mbps when the link was terminated. The data shows that there is a decline in throughput value of up to 71% due to the link termination to ISP 1.

Throughput value reduction was caused by data transfer process cessation when a failover from master router to slave router took a place. This condition could be the cause of several data packets loss, so that when a normal network

returned, a retransmission request occurred that resulting in an increase in the retransmission value. In addition, the decrease in throughput value was also caused by the data transmission lines transfer from the path to ISP 1 which had large bandwidth to ISP 2 with smaller bandwidth.

TABLE III
DELAY MEASUREMENT RESULTS

Test Number	Without Link Termination (ms)			With Link Termination (ms)		
	PDF	MKV	ISO	PDF	MKV	ISO
1	0.13	0.17	0.16	0.82	0.61	0.31
2	0.12	0.18	0.16	0.64	0.66	0.34
3	0.14	0.13	0.1	0.62	0.3	0.27
4	0.13	0.11	0.12	0.59	0.68	0.26
5	0.16	0.1	0.11	0.88	0.54	0.35
Average	0.14	0.14	0.13	0.71	0.56	0.31

The next test was parameter delay measurement. Parameter delay test aimed to determine average time delay between transmitted data packets from internet to client. The results of delay measurements are shown in Table III.

When file download by client was carried out without link termination, the obtained average delay was 0.14 ms for PDF file, 0.14 ms for MKV files, and 0.13 ms for ISO files, while the file download was carried out when there was a link termination the occurring delay was 0.71 ms for PDF files, 0.56 ms for MKV files, and 0.31 ms for ISO files. Average

delay value when downloading songs for those file types was 0.14 ms without link termination and 0.53 ms with a link termination. Based on these data, it could be seen that there was an increase in the delay value when the link termination took place. This happened because the link termination resulted in a failover process so that the data transfer was delayed. Nevertheless, the average delay value obtained from measurements in both conditions was less than 150 ms, so that based on the ITU-T G.114 standard it was still classified as good quality.

The QoS parameter that was measured next was retransmission. Retransmission measurements aimed to determine packet percentage that experiencing retransmission due to a failure in packets transmission and this mechanism occurred in packets using TCP protocol. Retransmission value measurements when downloading files from Google Drive were obtained from Wireshark recordings using the tcp.analysis.retransmission filter.

The retransmission process by the TCP protocol recorded on Wireshark showed retransmission from the address 74.125.200.94 which was Google's server address to the address 192.168.100.3 which was the client's IP address. The

Wireshark recordings are shown in Fig. 5, while the results of retransmission measurements are shown in Table IV.

TABLE IV
RETRANSMISSION MEASUREMENT RESULTS

Test Number	Without Link Termination (%)			With Link Termination (%)		
	PDF	MKV	ISO	PDF	MKV	ISO
1	1.2	1.7	1.8	1.5	1.4	1.3
2	1.3	1.4	1.6	2.5	1.3	1.4
3	1	1	0.20	1.3	1.7	0.30
4	0.3	0.2	1.5	1.7	1.2	1.1
5	1.7	1.8	1.4	1.6	2.2	2
Average	1.1	1.22	1	1.72	1.56	1.45

Based on Table IV, the average retransmission value when downloading files without link termination was 1.1% for PDF files, 1.22% for MKV files, and 1% for ISO files, while the average retransmission value when downloading files with link termination was 1.72% for PDF files, 1.56% for MKV files, and 1.45% for ISO files. The average retransmission value when downloading for these three file types was 1.11% without link termination and 1.58% when a link was terminated.

71290	36.258899	192.168.100.3	74.125.200.94	TLSv1.2	571	0.000889000 Client Hello
71291	36.266368	192.168.100.2	224.0.0.18	VRRP	70	Announcement (v2)
71292	36.337697	74.125.200.94	192.168.100.3	TCP	66	0.375541000 443 → 1529 [SYN, ACK] Seq=0 Ack=1 Win=
71293	36.337867	192.168.100.3	74.125.200.94	TCP	54	0.000170000 1529 → 443 [ACK] Seq=1 Ack=1 Win=66048
71294	36.739029	192.168.100.2	224.0.0.251	MDNS	139	Standard query response 0x0000 PTR, ca
71295	36.802841	74.125.200.94	192.168.100.3	TCP	66	0.543942000 [TCP Out-Of-Order] 443 → 1528 [SYN, AC
71296	36.803002	192.168.100.3	74.125.200.94	TCP	66	0.000161000 [TCP Dup ACK 71289#1] 1528 → 443 [ACK]
71297	36.803056	74.125.200.94	192.168.100.3	TCP	66	0.465189000 [TCP Retransmission] 443 → 1529 [SYN,
71298	36.803099	192.168.100.3	74.125.200.94	TCP	66	0.000043000 [TCP Dup ACK 71293#1] 1529 → 443 [ACK]

Fig. 5 TCP protocol retransmission.

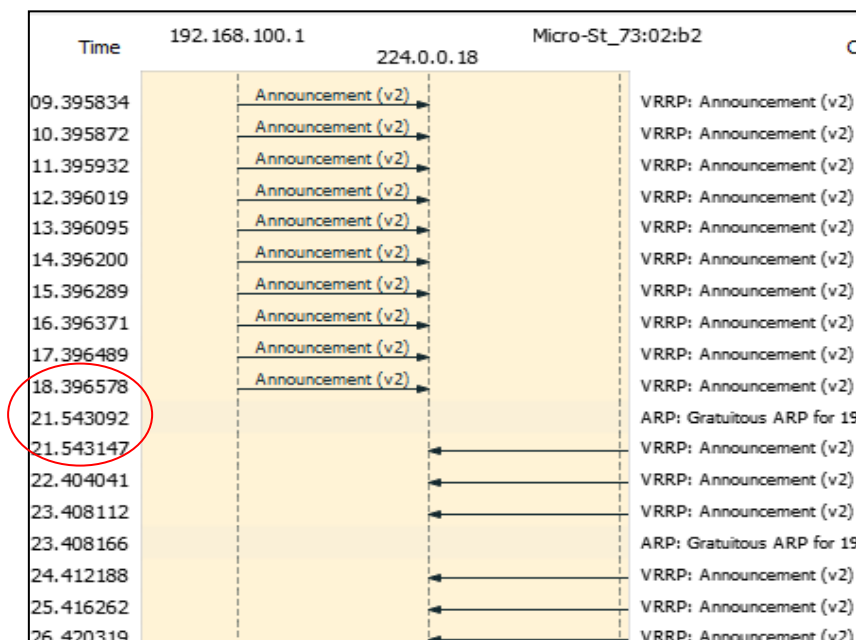


Fig. 6 Failover process flowchart display.

TABLE V
DOWNTIME VALUE MEASUREMENT

The condition Test Number	1				2				3			
	Master		Slave		Master		Slave		Master		Slave	
	1	1	100	1	0	1	1	1	0	1	1	1
1	5.72s (5 RTO)				4.23s (4 RTO)				3.05s (3 RTO)			
2	6.08s (5 RTO)				5.16s (4 RTO)				2.86s (2 RTO)			
3	5.64s (5 RTO)				5.09s (5 RTO)				2.84s (2 RTO)			
4	6.22s (5 RTO)				5.16s (4 RTO)				2.76s (2 RTO)			
5	6.45s (6 RTO)				5.16s (4 RTO)				2.68s (2 RTO)			
6	6.28s (6 RTO)				4.21s (3 RTO)				3.15s (3 RTO)			
7	6.30s (6 RTO)				5.15s (5 RTO)				2.51s (3 RTO)			
8	6.00s (5 RTO)				5.16s (5 RTO)				3.00s (3 RTO)			
9	5.69s (5 RTO)				5.15s (4 RTO)				3.16s (2 RTO)			
10	5.82s (7 RTO)				5.15s (4 RTO)				3.07s (2 RTO)			
Average Downtime	6.02 s				4.96 s				2.91 s			

Desc. ■ Deadratio=1 ■ Advskew ■ Advbase

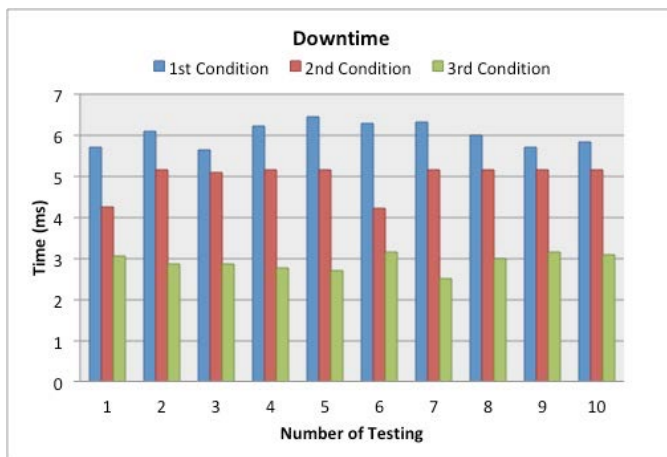


Fig. 7 Downtime value.

These results indicate that retransmission occurs either during normal network conditions or without link termination or when there is a link termination. In addition, the measured percentage retransmission value when a link termination occurs is greater than without the link termination. This is due to the packets transmission from the complex internet network to the client that allows transmission failure in the form of lost or damaged packages, so that a retransmission process is needed.

Next was measuring downtime value. Downtime values were measured to determine the duration when the network was down due to link termination to master router. When the network was down, a failover process occurred from the router master to the slave router so that the network could normally run again. The process could be recorded via Wireshark as shown in Fig. 6.

The amount of failover time was obtained from slave router (new master) initial advertisement time minus master router last advertisement time. Before the advertisement activity by the new router master continued, the ARP protocol would send broadcasts in an ARP gratuitous form. It was because

ARP gratuitous provided assistance in updating ARP table and informed all devices within the network about a fact that the slave router (new master) was virtual 192.168.100.254 IP address holder and performed its task as a master router.

In addition, deadratio, advskew, and advbase values of the CARP protocol on both routers were set to vary aimed to test the caused effect on downtime values. The downtime values measurement results are shown in Table V and the graphical form is shown in Fig. 7.

Before CARP protocol was implemented in the network, when link termination occurred, downtime in network could not be determined and client could not access network services for an indefinite period of time. After the CARP protocol was implemented, the downtime value could be minimized.

Based on the data in Table V, it can be seen that the average downtime value in the first condition was 6.02 s, the second condition was 4.96 s, and the third condition was 2.91 s. The lowest downtime value was obtained at condition 3, which was when the advskew, advbase, and deadratio values on the master router were equal to 0, 1, and 1, while the advskew, advbase, and deadline values in slave routers were all 1. Average downtime value reduction at condition 3 to 2.91 s was affected by the deadratio parameter = 1 so that it sped up the failover time on the router. Basically, deadratio parameter is length of time the slave router waits for the master router to not respond until it is deemed unavailable.

The downtime value of 2.91 s obtained in this paper is shorter than the downtime value in previous studies [5], [6].

V. CONCLUSION

The conclusion of this paper is that the CARP protocol implementation was successfully implemented on the constructed network. Based on the QoS parameters measurement results, the obtained values of throughput, delay, and retransmission are 61.7 Mbps, 0.14 ms, and 1.11% without link termination and 18 Mbps, 0.53 ms, and 1.58% when with link termination. The QoS test results are in the

good quality category according to the ITU-T standard. It shows that CARP implementation on the network can increase network availability and reliability when there is a link termination because failover process can take place shorter with an average value of downtime of 2.91 seconds.

ACKNOWLEDGEMENTS

Gratitude is bestowed to the DRPM Directorate General of Higher Education for funding assistance in the Higher Education Superior Basic Research (PDUPT) scheme in 2018 so that this research can be well administered.

REFERENCES

- [1] (2016) "It's Time to Become the Principal of Government and Industry Attention," [Online], [https://apjii.or.id/downfile/file/BULETINAPJII EDISI05November2016.pdf](https://apjii.or.id/downfile/file/BULETINAPJII%20EDISI05November2016.pdf), access date: 11-Dec-2017.
- [2] J.N.P. Soon, S.H.R. Abdulla, C.P. Yin, W.S. Wan, P.K. Yuen, and L.E. Heng, "Implementing of Virtual Router Redundancy Protocol in a Private University," *J. Ind. Intell. Inf.*, Vol. 1, No. 4, pp. 255–259, 2013.
- [3] P.T. Pribadi, "Implementasi High-Availability VPN Client Pada Jaringan Komputer Fakultas Hukum Universitas Udayana," *Jur. Ilmu Komput.*, Vol. 6, No. 1, pp. 17–24, 2013.
- [4] Tolqabaqci (2017) "What is Network Redundancy in Computer Networking?," [Online], <https://www.sysnettechsolutions.com/en/cisco/network-redundancy-in-computer-networking/>, access date: 11-Dec-2017.
- [5] A.I. Lesmana and Y.M. Sinaga, "Analisis Unjuk Kerja Implementasi Virtual Router Redundancy Protocol (VRRP) dan Common Address Redundancy Protocol (CARP) pada Jaringan Client-Server," Thesis, Universitas Indonesia, Jakarta, Indonesia, 2013.
- [6] A.D. Lumingkewas, A.S.M. Lumenta, and X.B.N. Najoran, "Perancangan dan Implementasi Gateway Redundancy untuk Peningkatan Reliabilitas Jaringan Menggunakan Protokol CARP," *E-Journal Teknik Elektro dan Komputer*, Vol. 5, No. 4, pp. 8–17, 2016.
- [7] V. Veselý, J. Holuša, and O. Ryšavý, "First-hop Redundancy Protocols in Omnet++," *Proceedings of the 7th International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH 2017)*, 2017, pp. 331–339.
- [8] F. Koch and K.T. Hansen, "Redundancy Performance of Virtual Network Solutions," *IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA*, 2006, pp. 328–332.
- [9] S. Institute, "CARP-The Free Fail-over Protocol," *Glob. Inf. Assur. Certif. Pap.*, 2005, pp. 1–16.
- [10] F. Denis (2013) "UCARP," [Online], <https://github.com/jedisct1/UCarp>, access date: 03-Apr-2017.
- [11] J. Stoklasa (2015) "CARP as HA solution in VMware Environments," [Online], <https://www.stoklasa.one/carp-in-vi/>, access date: 03-Apr-2017.
- [12] M.Y. Choirullah, M. Anif, and A. Rochadi, "Analisis Kualitas Layanan Virtual Router Redundancy Protocol Menggunakan Mikrotik pada Jaringan VLAN," *JNTETI*, Vol. 5, No. 4, pp. 278–285, 2016.
- [13] R.S. Herdiansyah, "Analisis Perbandingan Quality of Service Load Balancing Menggunakan Metode NTH dan PCC (Per Connection Classifier)," Thesis, Universitas Widyatama, Bandung, Indonesia, 2015.
- [14] R.S. Lubis and M. Pinem, "Analisis Quality of Service (QoS) Jaringan," *Singuda Ensikom*, Vol. 7, No. 3, pp. 131–136, 2014.
- [15] Alamsyah, E. Setijadi, I.K.E. Purnama, and M.H. Purnomo, "Analisis Kinerja Protokol Routing Reaktif dan Proaktif pada MANET Menggunakan NS2," *JNTETI*, Vol. 7, No. 2, pp. 138–143, 2018.
- [16] Irfani, "Implementasi High Availability Server dengan Failover Virtual Computer Cluster," Thesis, Universitas Muhammadiyah Surakarta, Surakarta, Indonesia, 2015.